CLAIMS

What is claimed is:

Sub a1

1. A method for remotely monitoring the operation of a communication device, comprising the steps of:

receiving a communication at the communication device;

determining whether the communication comprises a security risk; and

in response to determining that the communication comprises a security risk, transmitting an alert signal to a remote monitoring center.

2. The method of Claim 1, wherein the determining step comprises comparing the communication to a plurality of known security risks to determine if the communication comprises one of the plurality of known security risks.

3. The method of Claim 2, wherein the determining step further comprises classifying the communication as a high priority event or a low priority event based upon the comparison.

4. The method of Claim 3, further comprising the steps of:

in response to classifying the communication as a high priority event, determining whether the communication should be terminated; and

in response to determining that the communication should be terminated, terminating the communication of the communication device.

5. The method of Claim 1, further comprising the steps of:

receiving the alert signal at the remote monitoring center; and

in response to receiving the alert signal, assigning a priority to the alert signal based upon a type of the communication.

6. The method of Claim 5, further comprising the step of forwarding the alert signal to a monitoring agent based upon the assigned priority of the alert signal.

7. The method of Claim 6, further comprising the steps of:

receiving the alert signal at the monitoring agent;

resolving a resolution to the communication causing the alert signal; and

contacting a user of the communication device with the resolution to the alert signal based on the analysis of the communication.

8. A method for remotely configuring a communication device, comprising the steps of:

determining a network address for the communication device;

transmitting a wake-up signal, comprising the network address from the communication device to a remote computer; and

in response to receiving the wake-up signal, transmitting configuration information from the remote computer to the communication device at the network address.

9. The method of Claim 8, further comprising the step of activating the communication device and implementing a plurality of security policies within the communication device for identifying security risks at the communication device.

10. The method of Claim 8, wherein the step of transmitting the wake-up signal comprises the steps of:

transmitting a first identification number and a network address via an encrypted communications channel;

receiving the first identification number and the network address at the remote computer; and

recording the first identification number and the network address in a first database at the remote computer.

11. The method of Claim 10, further comprising the steps of:

transmitting a plurality of diagnostic variables from the communication device to the remote computer via the encrypted communications channel;

receiving the diagnostic variables at the remote computer; and

determining whether the communication device is functioning properly based upon the diagnostic variables.

12. The method of Claim 10, further comprising the steps of:

transmitting status information along with the first identification number and the network address via the encrypted communications channel;

receiving the status information at the remote computer;

recording the status information in the first database; and

determining whether the communication device meets a plurality of operational requirements based upon the status information.

13. The method of Claim 12, wherein the step of determining whether the communication device meets a plurality of operational requirements further comprises the steps of:

determining whether the communication device requires a software patch based upon the status information; and

in response to determining that the communication device requires the software patch, transmitting the software patch to the communication device.

14. The method of Claim 13, wherein the step of transmitting the software patch comprises the steps of:

moving the software patch to a queue in response to determining that the communication device requires a software patch; and

transmitting the queued software patch to the communication device in response to receiving configuration information.

15. The method of Claim 14, wherein the software patch is transmitted to the communication device via an encrypted communications channel.

16. The method of Claim 15, further comprising the steps of:

receiving the software patch at the communication device;

applying the software patch to the communication device; and

transmitting a configuration complete signal from the new communication device to the remote computer.

17. The method of Claim 16, further comprising the steps of:

receiving the configuration complete signal at the remote computer;

performing a vulnerability analysis on the communication device;

determining whether the vulnerability analysis failed; and

in response to determining that the vulnerability analysis failed, requesting modified configuration information.

18. A method for remotely configuring a communication device, comprising the steps of:

transmitting a first identification number and a network address via an encrypted communications channel;

receiving the first identification number and the network address at the remote computer;

recording the first identification number and the network address in a first database at the remote computer, wherein the network address is associated with the first identification number;

receiving a request to configure the communication device comprising a second identification number at the remote computer;

matching the second identification number to a first identification number stored in the first database; and

in response to matching the second number to the first number, transmitting configuration information to the communication device at the network address.

19. The method of Claim 18, further comprising the steps of:

determining whether the second identification number is valid by comparing the second identification number with the first identification number in the first database; and

in response to determining that the second identification number is valid, receiving a control input.

20. The method of Claim 19, wherein the step of receiving the control input comprises the steps of:

displaying a plurality of configuration options; and

receiving a control input selecting one of the plurality of configuration options as a selected option.

21. The method of Claim 19, further comprising the step of determining whether the selected option comprises a request to configure a new communication device.

22. The method of Claim 21, further comprising the steps of:

in response to determining that the selected option comprises a request to configure a new communication device, receiving configuration information for the communication device comprising at least one billing parameter corresponding to a user of the communication device; and

transmitting initiation information to the communication device.

23. The method of Claim 22, wherein the step of transmitting the initiation information comprises the step of transmitting a correct time, a download queue, and an activation code, to the communication device via an encrypted communications channel.

24. The method of Claim 22, further comprising the step of notifying a user of the communication device that the communication device is active.

25. The method of Claim 22, further comprising the steps of:

receiving a configuration complete signal at the remote computer;

performing a vulnerability analysis on the communication device;

determining whether the vulnerability analysis failed; and

in response to determining that the vulnerability analysis failed, requesting modified configuration information.

26. The method of Claim 19, further comprising the step of determining whether the selected option comprises a request to modify a configuration of the communication device.

27. The method of Claim 26, further comprising the steps of:

in response to determining the selected option comprises a request to modify a configuration, receiving the modified configuration information; and

transmitting the modified configuration information to the communication device.

28. The method of Claim 27, wherein the step of transmitting the modified configuration information comprises the step of transmitting security policy information to the communication device via an encrypted communications channel.

29. The method of Claim 28, further comprising the step of notifying a user of the communication device that the communication device is active.

30. A system for remotely monitoring a communication device comprising:

a communication device; and

a remote monitoring center,

and wherein the communication device is operative to receive a communication , determine whether the communication comprises a security risk, and transmit an alert signal to the remote monitoring center upon determination that the communication comprises a security risk,

and wherein the remote monitoring center is operative to receive the alert signal, assign a priority on the alert signal, transmit the alert signal to a monitoring agent based upon the assigned priority, analyze the communication, and transmit a resolution to a user of the communication device.

31. A method for remotely configuring and monitoring a communication device, comprising the steps of:

determining a network address for the communication device;

transmitting a wake-up signal, comprising the network address from the communication device to a remote computer;

in response to receiving the wake-up signal, transmitting configuration information from the remote computer to the communication device at the network address;

activating the communication device to implement a plurality of security options within the communication device for identifying security risks at the communication device;

receiving a request to configure the communication device at the remote computer;

in response to receiving the request to configure, receiving configuration information for the communication device comprising at least one billing parameter corresponding to a user of the communication device;

transmitting initiation information to the communication device;

in response to receiving the initiation information, initiating remote monitoring of the communication device;

in response to initiating remote monitoring, performing a vulnerability analysis on the communication device;

determining whether the vulnerability analysis failed;

in response to determining that the vulnerability analysis failed, requesting modified configuration information and in response to determining the vulnerability analysis passed, continue remote monitoring of the communication device;

receiving a communication at the communication device;

determining whether the communication comprises a security risk;

in response to determining that the communication comprises a security risk, transmitting an alert signal to a remote monitoring center;

receiving the alert signal at the remote monitoring center;

forwarding the alert signal to a monitoring agent;

receiving the alert signal at the monitoring agent;

analyzing the communication; and

contacting a user of the communication device with an appropriate resolution to the alert signal based on the analysis of the communication.

32. A communication device, comprising:

a processor; wherein the processor determines a network address for the communication device;

a transmitter; wherein the transmitter sends a wake-up signal, comprising the network address from the communication device to a remote computer;

a receiver, wherein the receiver receives a communication;

in response to receiving the communication, the processor determining whether the communication comprises a security risk; and

in response to determining the communication comprises a security risk, the transmitter transmitting an alert signal to a remote monitoring center.

33. A method for receiving an alert signal indicative of an attack and resolving the attack, comprising the steps of:

receiving the alert signal at a remote monitoring center;

logging the information contained in the alert signal in a database;

assigning an order preference to the alert signal based upon the type of attack causing the alert signal;

forwarding the alert signal to a remote agent based upon the order preference; and

analyzing and resolving the attack.

34. The method of Claim 33, wherein the receiving step comprises receiving a first packet comprising the attack causing the alert signal and a priority level associated with the attack.

35. The method of Claim 34, wherein the receiving step further comprises receiving a second packet comprising information indicative of the specific intrusion rule the attack violated.

36. The method of Claim 33, wherein before performing the logging step, the database is selected from a plurality of databases based upon an assigned priority of the alert signal.

37. A remote monitoring center for receiving an alert signal indicative of an attack and resolving the attack, comprising:

a receiver, wherein the receiver receives the alert signal;

a recorder, wherein the recorder logs the information contained in the alert signal in a first database;

a prioritizer, wherein the prioritizer assigns an order preference to the alert signal based upon the type of attack causing the alert signal;

a transmitter, wherein the transmitter forwards the alert signal based upon the order preference; and

a remote agent, where in the remote agent analyzes and resolves an appropriate resolution to the attack.

38. A method for determining an attack and transmitting an alert signal, comprising the steps of:

receiving a communication at a communication device;

comparing the communication with a list of known attacks;

determining whether the communication matches one of the known attacks; and

in response to determining the communication matches one of the known attacks, transmitting an alert signal to a remote monitoring center.

39. The method of Claim 38, wherein the comparing step further comprises the steps of:

disassembling the communication to determine the communication's header information; and

comparing the communication's header information to entries in a table comprising header information of known attacks.

40. The method of Claim 39, further comprising the steps of:

disassembling the communication to determine the communication's body information;

comparing the communication's body information to entries in a table comprising body information of known attacks;

determining which one of the known attacks the communication matches; and

transmitting a packet to the remote monitoring center, wherein the packet informs the remote monitoring center which attack the communication matches.